UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/538,289	06/10/2005	Michiaki Tatsubori	JP920020206US1	9237

47069 7590 04/01/2008
KONRAD RAYNES & VICTOR, LLP
ATTN: IBM54
315 SOUTH BEVERLY DRIVE, SUITE 210
BEVERLY HILLS, CA 90212

EXAMINER	
TURNER, ASHLEY D	
ART UNIT	PAPER NUMBER
2154	
MAIL DATE	DELIVERY MODE
04/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/538,289	**Applicant(s)** TATSUBORI ET AL.
	Examiner ASHLEY D. TURNER	**Art Unit** 2154

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 June 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-39* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 21-39 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Schneider (U.S. 6,785,728 B1), in view of Ross et al (US 6,629,135 B1).

Referring to claim 21 Schneider discloses a system for providing services; comprising a computer; a storage section storing execution results for a previous execution of objects; code executed by the computer to perform operations, the operations comprising receiving a call request with respect to an object and a user identifier; comparing access authority for the user identifier and an access authority set for methods that may be called with respect to the object (Col.9 lines 40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which data base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information resources 320, which defines the individual information items subject to protection and specifies where to find them; information sets 321, which defines groups of information resources); and Schneider did not disclose transmitting execution results for the previous execution of the object prior to executing the call request with respect to the object in response to determining that the storage section stores the execution results for the object subject to the call request. The general concept of transmitting execution results for the previous execution of the object prior to executing the call request with respect to the object in response to determining that the storage section stores the execution results for the object subject to the call request is well known in the art as taught by Ross. Ross discloses transmitting execution results for the previous execution of the object prior to executing the call request with respect to the object in response to determining that the storage section stores the execution results for the object subject to the call request. (Col 5 lines 56-61 Object Cache 250. The object cache contains the responses to previously submitted requests. All items in the cache are marked with an expiration time that is set at the time they are originally retrieved. The purpose of this layer is to reduce the load on the application tier). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify

Schneider to include transmitting execution results for the previous execution of the object prior to executing the call request with respect to the object in response to determining that the storage section stores the execution results for the object subject to the call request in order to provide its Hosts with the added value and incremental revenues of traditional affiliate programs, but the company also enables Hosts to control the customer experience before, during, and after the purchase transaction.

Referring to claim 22

Referring to claim 22 Schneider and Ross disclose all the limitations of claim 22 which is described above. Schneider also discloses wherein the call request is received over a network (Col. 2 lines 6-24 FIG. 1 shows techniques presently used to increase security in networks that are accessible via the Internet. FIG. 1 shows network 101, which is made up of two separate internal networks 103(A) and 103(B) that are connected by Internet 111. Networks 103(A) and 103(B) are not generally accessible, but are part of the Internet in the sense that computer systems in these networks have Internet addresses and employ Internet protocols to exchange information. Two such computer systems appear in FIG. 1 as requestor 105 in network 103(A) and server 113 in network 103(b). Requestor 105 is requesting access to data which can be provided by server 113. Attached to server 113 is a mass storage device 115 that contains data 117 which is being requested by requester 105. Of course, for other data, server 113 may be the requester and requestor 105 the server. Moreover, access is to be understood in the present context as any operation which can read or change data stored on server 113 or which can change the state of server 113. In making the request, requestor 105 is using one of the standard TCP/IP protocols, wherein the execution results are transmitted over the network, wherein the call request with respect to the object comprises for Web services. (Col. 21 lines 20-37 b. For segment (b), if the weakest trust level of any network component in the path is greater than or equal to the data sensitivity of the resource, then the traffic is sent without encryption. This corresponds to the case where the network is inherently secure enough to transmit the data. In the example table above, information resources with a Public data sensitivity level may be transmitted on any network, as shown by row 609(4). However, the access filters 203 will use SKIP to authenticate the session, allowing subsequent access filters to pass the session through without incurring the larger overheads of decryption, access checking, and reencryption. If the weakest trust level for the path is less than the data sensitivity of the resource, then the SEND table is consulted for the minimum encryption algorithm required for the sensitivity level and the session is encrypted using that algorithm. The encryption upgrades the security of the link, making it suitable to carry data of that given sensitivity and permitting access by the user to the resource).

Referring to claim 23

Referring to claim 23 Schneider and Ross disclose all the limitations of claim 23 which is described above. Schneider also discloses searching the storage section for execution results for the object subject to the call request in response to determining that the access authority for the user identifier is contained in the access authority set. (Col. 26 lines 27-40 The IntraMap interface lets the user sort Resource List 1803 by information sets, locations, or services. To do this, the user selects the way he or she wishes to sort the resource list in sort field 1809. The user may also specify the order in which the categories are used in the sort. The interface further has a search function. To do a search, the user enters a search string in FIND field 1807. The resource list and the resource descriptions for the resources on it are then searched in the order specified in sort field 1809. The search simply looks for whole or partial word matches. It is not case sensitive. The first match is displayed, and function keys may be used to navigate to other matches. Of course, if a user has not checked a service type in service type field 1811, resources of that service type are not involved in either sorting or searching.)

Referring to claim 24

Referring to claim 24 Schneider and Ross disclose all the limitations of claim 24 which is described above. Schneider also discloses an object execution component executed by the computer, wherein if the storage section does not contain execution results for the object subject to the call request, then the call request is transmitted to the object execution component to execute the call request with respect to the object. (Col. 27 lines 49-67 and Col.28 lines 1-11 When the request is received in access filter 203(c), IP filter 2419 forwards it to Web proxy 2421, which in turn forwards it to Web server 2423, which responds to the request by downloading IntraMap applet 2411 to Web browser 2429 in work station 2403, where IntraMap applet 2411 begins executing in Web browser 2429. During execution, it sends a request to IntraMap proxy 2427 for IntraMap information 2422. Like all Java applets, IntraMap applet 2411 sends the request to the server that it is resident on, in this case, access filter 203(c). However, as with any other request from workstation 2403, the request goes by way of local access filter 203(I). There, IntraMap proxy 2427 detects that the request is addressed to IntraMap proxy 2427 in access filter 203(c) and instead of sending the request on to access filter 203(c), obtains IntraMap information 2422 from the local copy of access control data base 301 in local access filter 203(I), filters it so that it specifies only those resources belonging to the information sets to which the user groups to which the user belongs have access to make to list 2431 and returns it via LAN 213 to IntraMap applet 2411, which then uses list 2431 to make IntraMap display 1801. In making the display, applet 2411 applies any filters specified in the request and also sorts the list as specified in the request. List 2431 not only indicates the resources that are available, but also contains information needed to fetch the resource. Thus, if the resource has a hyperlink, the hyperlink is included in the list, if it is a resource for which the user presently does not have access, but to which the user may request access, the list includes the name and email address of the administrator for the resource.)

Referring to claim 25

Referring to claim 25 Schneider and Ross disclose all the limitations of claim 25 which is described above. Schneider also discloses wherein the computer includes an edge server that performs the operations of receiving the call request and comparing the access authority for the user identifier, and wherein an application server implements the object execution component. (Col. 2 lines 6-24 FIG. 1 shows techniques presently used to increase security in networks that are accessible via the Internet. FIG. 1 shows network 101, which is made up of two separate internal networks 103(A) and 103(B) that are connected by Internet 111. Networks 103(A) and 103(B) are not generally accessible, but are part of the Internet in the sense that computer systems in these networks have Internet addresses and employ Internet protocols to exchange information. Two such computer systems appear in FIG. 1 as requestor 105 in network 103(A) and server 113 in network 103(b). Requestor 105 is requesting access to data which can be provided by server 113. Attached to server 113 is a mass storage device 115 that contains data 117 which is being requested by requester 105. Of course, for other data, server 113 may be the requester and requestor 105 the server. Moreover, access is to be understood in the present context as any operation which can read or change data stored on server 113 or which can change the state of server 113. In making the request, requestor 105 is using one of the standard TCP/IP protocols. As used here, a protocol is a description of a set of messages that can be used to exchange information between computer systems. The actual messages that are sent between computer systems that are communicating according to a protocol are collectively termed a session. During the session, Requestor 105 sends messages according to the protocol to server 113's Internet address and server 113 sends messages according to the protocol to requester 105's Internet address. Both the request and response will travel between internal network 103(A) and 103(B) by Internet 111. If server 113 permits requestor 105 to access the data, some of the messages flowing from server 113 to requestor 105 in the session will include the requested data 117. The software components of server 113 which respond to the messages as required by the protocol are termed a service.)

Referring to claim 26

Referring to claim 26 Schneider discloses a computer; a storage section storing execution results for a previous execution of objects ; components executed by the computer to perform operations (Col. 2 lines 6-24 FIG. 1 shows techniques presently used to increase security in networks that are accessible via the Internet. FIG. 1 shows network 101, which is made up of two separate internal networks 103(A) and 103(B) that are connected by Internet 111. Networks 103(A) and 103(B) are not generally accessible, but are part of the Internet in the sense that computer systems in these networks have Internet addresses and employ Internet protocols to exchange information. Two such computer systems appear in FIG. 1 as requestor 105 in network 103(A) and server 113 in network 103(b). Requestor 105 is requesting access to data which can be provided by server 113. Attached to server 113 is a mass storage device 115 that contains data 117 which is being requested by requester 105. Of course, for other data, server 113 may be the requester and requestor 105 the server. Moreover, access is to be understood in the present context as any operation which can read or change data stored on server 113 or which can change the state of server 113. In making the request, requestor 105 is using one of the standard TCP/IP protocols. As used here, a protocol is a description of a set of messages that can be used to exchange information between computer systems. The actual messages that are sent between computer systems that are communicating according to a protocol are collectively termed a session. During the session, Requestor 105 sends messages according to the protocol to server 113's Internet address and server 113 sends messages according to the protocol to requester 105's Internet address. Both the request and response will travel between internal network 103(A) and 103(B) by Internet 111. If server 113 permits requestor 105 to access the data, some of the messages flowing from server 113 to requestor 105 in the session will include the requested data 117. The software components of server 113 which respond to the messages as required by the protocol are termed a service.), comprising: an object analyzer generating an access authority sets for methods that may be called (Col. 48 lines 48-53 The access filter analyzes the trust levels of the network segments between the user and the server that contains the information item, and any of them is lower than the information item's sensitivity, the access filter requires that the session be encrypted with an encryption algorithm whose trust level is at least as high as the information item's sensitivity level.); Schneider did not disclose an object executor for executing a call request from a user with respect to an object; and a cache mechanism configured to store execution results for the previous execution of the object subject to the call request and to use the access authority set to determine whether a user issuing the call request has authority to access, from the storage section, the previous execution of the object subject to the call request. The general concept of an object executor for executing a call request from a user with respect to an object; and a cache mechanism configured to store execution results for the previous execution of the object subject to the call request and to use the access authority set to determine whether a user issuing the call request has authority to access, from the storage section, the previous execution of the object subject to the call request is well known in the art as taught by Ross. Ross discloses an object executor for executing a call request from a user with respect to an object; and a cache mechanism configured to store execution results for the previous execution of the object subject to the call request and to use the access authority set to determine whether a user issuing the call request has authority to access, from the storage section, the previous execution of the object subject to the call request (Col 5 lines 56-61 Object Cache 250. The object cache contains the responses to previously submitted requests. All items in the cache are marked with an expiration time that is set at the time they are originally retrieved. The purpose of this layer is to reduce the load on the application tier).

Referring to claim 27

Referring to claim 27 Schneider and Ross disclose all the limitations of claim 27 which is described above. Ross also discloses wherein the cache mechanism further includes: a request manager; and an access controller for controlling a search for execution results for on previous execution of the object stored in the storage section to return the previous execution of the object in response to the call request. (Col 5 lines 56-61 Object Cache 250. The object cache contains the responses to previously submitted requests. All items in the cache are marked with an expiration time that is set at the time they are originally retrieved. The purpose of this layer is to reduce the load on the application tier).

Referring to claim 28

Referring to claim 28 Schneider and Ross disclose all the limitations of claim 28 which is described above. Schneider also discloses wherein the access controller compares an access authority for the user initiating the call request and the access authority set to perform access control; and wherein the request manager passes the object call request to the object executor to control execution of the call request with respect to the object in response to the access controller determining that the user initiating the call request has access authority. (Col.9 lines 40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which data base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information resources 320, which defines the individual information items subject to protection and specifies where to find them; information sets 321, which defines groups of information resources)

Referring to claim 29

Referring to claim 29 Schneider and Ross disclose all the limitations of claim 29 which is described above. Schneider also discloses wherein the object analyzer is further executed to perform acquiring a method which may be called by the object(Col. 48 lines 48-53 The access filter analyzes the trust levels of the network segments between the user and the server that contains the information item, and any of them is lower than the information item's sensitivity, the access filter requires that the session be encrypted with an encryption algorithm whose trust level is at least as high as the information item's sensitivity level.); acquiring access authority corresponding to the method; and generating the access authority set from access authority for all methods which may be called by the object. (Col.9 lines 40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which data base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information resources 320, which defines the individual information items subject to protection and specifies where to find them; information sets 321, which defines groups of information resources)

Referring to claim 30

Referring to claim 30 Schneider and Ross disclose all the limitations of claim 30 which is described above. Schneider also discloses wherein the cache mechanism comprises an edge server and the object analyzer comprises an application server. (Col. 48 lines 48-68 and Col.49 lines 1-3 The access filter also assigns trust levels to segments of the actual networks in virtual private network 201 and to encryption algorithms. The access filter analyzes the trust levels of the network segments between the user and the server that contains the information item, and any of them is lower than the information item's sensitivity, the access filter requires that the session be encrypted with an encryption algorithm whose trust level is at least as high as the information item's sensitivity level. If a segment between the user and the first access filter or a segment between the last access filter and the server does not have the requisite trust level, the first access filter requires that the user or server encrypt the session with an encryption algorithm that has the requisite trust value before it will allow access, if a subsetment of the segment between the first access filter and the last access filter, the first access filter itself encrypts the session using an encryption algorithm that has the requisite trust level. By requiring only the trust level necessary for an information item's sensitivity, the access filter reduces the burden of access checking to what is actually required for the information item; by permitting the user to offer a more trustworthy identification and using encryption to upgrade the trustworthiness of a segment of the network, the access filter provides flexibility without compromising security. It should be noted that in other embodiments, the first access filter may encrypt the session as required for the server, providing of course that the encryption for the server is sufficient for the trust level of the resource.)

Referring to claim 31

Referring to claim 31 Schneider discloses receiving a call request with respect to an object; acquiring access authority for the object; determining whether the access authority is contained in the access authority set (Col.9 lines 40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which data base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information resources 320, which defines the individual information items subject to protection and specifies where to find them; information sets 321, which defines groups of information resources); and searching a storage section storing execution results for a previous execution of the object prior to executing the call request and in response to determining that the access authority is contained in the access authority set (Col. 26 lines 27-40 The IntraMap interface lets the user sort Resource List 1803 by information sets, locations, or services. To do this, the user selects the way he or she wishes to sort the resource list in sort field 1809. The user may also specify the order in which the categories are used in the sort. The interface further has a search function. To do a search, the user enters a search string in FIND field 1807. The resource list and the resource descriptions for the resources on it are then searched in the order specified in sort field 1809. The search simply looks for whole or partial word matches. It is not case sensitive. The first match is displayed, and function keys may be used to navigate to other matches. Of course, if a user has not checked a service type in service type field 1811, resources of that service type are not involved in either sorting or searching). Schneider did not disclose reading an access authority set for execution of the call request with respect to the object. The general concept of reading an access authority set for execution of the call request with respect to the object is well known in the art as taught by Ross. Ross discloses reading an access authority set for execution of the call request with respect to the object (Col 5 lines 56-61 Object Cache 250. The object cache contains the responses to previously submitted requests. All items in the cache are marked with an expiration time that is set at the time they are originally retrieved. The purpose of this layer is to reduce the load on the application tier). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Schneider to include reading an access authority set for execution of the call request with respect to the object in order to provide its Hosts with the added value and incremental revenues of traditional affiliate programs, but the company also enables Hosts to control the customer experience before, during, and after the purchase transaction.

Referring to claim 32

Referring to claim 32 Schneider and Ross disclose all the limitations of claim 32 which is described above. Schneider also discloses wherein the call request is received over a network, and wherein the execution results are transmitted over the network and wherein the call request with respect to the object comprises a request for Web services. (Col. 2 lines 6-24 FIG. 1 shows techniques presently used to increase security in networks that are accessible via the Internet. FIG. 1 shows network 101, which is made up of two separate internal networks 103(A) and 103(B) that are connected by Internet 111. Networks 103(A) and 103(B) are not generally accessible, but are part of the Internet in the sense that computer systems in these networks have Internet addresses and employ Internet protocols to exchange information. Two such computer systems appear in FIG. 1 as requestor 105 in network 103(A) and server 113 in network 103(b). Requestor 105 is requesting access to data which can be provided by server 113. Attached to server 113 is a mass storage device 115 that contains data 117 which is being requested by requester 105. Of course, for other data, server 113 may be the requester and requestor 105 the server. Moreover, access is to be understood in the present context as any operation which can read or change data stored on server 113 or which can change the state of server 113. In making the request, requestor 105 is using one of the standard TCP/IP protocols. As used here, a protocol is a description of a set of messages that can be used to exchange information between computer systems. The actual messages that are sent between computer systems that are communicating according to a protocol are collectively termed a session. During the session, Requestor 105 sends messages according to the protocol to server 113's Internet address and server 113 sends messages according to the protocol to requester 105's Internet address. Both the request and response will travel between internal network 103(A) and 103(B) by Internet 111. If server 113 permits requestor 105 to access the data, some of the messages flowing from server 113 to requestor 105 in the session will include the requested data 117. The software components of server 113 which respond to the messages as required by the protocol are termed a service.)

Referring to claim 33

Referring to claim 25 Schneider and Ross disclose all the limitations of claim 25 which is described above. Ross also discloses transmitting the execution results for the previous execution of the object prior to executing the call request with respect to the object in response to determining that the storage section stores the execution results for the previous execution of the object subject to the call request. (Col 5 lines 56-61 Object Cache 250. The object cache contains the responses to previously submitted requests. All items in the cache are marked with an expiration time that is set at the time they are originally retrieved. The purpose of this layer is to reduce the load on the application tier).

Referring to claim 34

Referring to claim 34 Schneider and Ross disclose all the limitations of claim 34 which is described above. Schneider also discloses passing the call request to an object executor in response to determining that the storage section does not store execution results for the previous execution of the object subject to the call request. (Col.9 lines 40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which data base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information resources 320, which defines the individual information items subject to protection and specifies where to find them; information sets 321, which defines groups of information resources)

Referring to claim 35

Referring to claim 35 Schneider also discloses a computer readable medium including instructions that when executed cause a computer to interact with a storage section and to perform operations comprising: receiving a call request with respect to an object; acquiring access authority for the object; reading an access authority set for execution of the object (Col. 2 lines 6-24 FIG. 1 shows techniques presently used to increase security in networks that are accessible via the Internet. FIG. 1 shows network 101, which is made up of two separate internal networks 103(A) and 103(B) that are connected by Internet 111. Networks 103(A) and 103(B) are not generally accessible, but are part of the Internet in the sense that computer systems in these networks have Internet addresses and employ Internet protocols to exchange information. Two such computer systems appear in FIG. 1 as requestor 105 in network 103(A) and server 113 in network 103(b). Requestor 105 is requesting access to data which can be provided by server 113. Attached to server 113 is a mass storage device 115 that contains data 117 which is being requested by requester 105. Of course, for other data, server 113 may be the requester and requestor 105 the server. Moreover, access is to be understood in the present context as any operation which can read or change data stored on server 113 or which can change the state of server 113. In making the request, requestor 105 is using one of the standard TCP/IP protocols. As used here, a protocol is a description of a set of messages that can be used to exchange information between computer systems. The actual messages that are sent between computer systems that are communicating according to a protocol are collectively termed a session. During the session, Requestor 105 sends messages according to the protocol to server 113's Internet address and server 113 sends messages according to the protocol to requester 105's Internet address. Both the request and response will travel between internal network 103(A) and 103(B) by Internet 111. If server 113 permits requestor 105 to access the data, some of the messages flowing from server 113 to requestor 105 in the session will include the requested data 117. The software components of server 113 which respond to the messages as required by the protocol are termed a service.); determining whether the access authority is contained in the access authority set (Col. 48 lines 48-53 The access filter analyzes the trust levels of the network segments between the user and the server that contains the information item, and any of them is lower than the information item's sensitivity, the access filter requires that the session be encrypted with an encryption algorithm whose trust level is at least as high as the information item's sensitivity level.); Schneider did not disclose searching the storage section which stores execution results for a previous execution of the object in response to determining that the access authority is contained in the access authority set prior to executing the call request with respect to the object. The general concept of searching the storage section which stores execution results for a previous execution of the object in response to determining that the access authority is contained in the access authority set prior to executing the call request with respect to the object is well known in the art as taught by Ross. Ross discloses searching the storage section which stores execution results for a previous execution of the object in response to determining that the access authority is contained in the access authority set prior to executing the call request with respect to the object (Col 5 lines 56-61 Object Cache 250. The object cache contains the responses to previously submitted requests. All items in the cache are marked with an expiration time that is set at the time they are originally retrieved. The purpose of this layer is to reduce the load on the application tier). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Schneider to include searching the storage section which stores execution results for a previous execution of the object in response to determining that the access authority is contained in the access authority set prior to executing the call request with respect to the object in order to in order to provide its Hosts with the added value and incremental revenues of traditional affiliate programs, but the company also enables Hosts to control the customer experience before, during, and after the purchase transaction.

Referring to claim 36

Referring to claim 36 Schneider and Ross disclose all the limitations of claim 36 which is described above. Schneider also discloses wherein the call request is received over a network, wherein the operations further comprise: transmitting the execution results over the network and wherein the call request with respect to the object comprises a request for Web services. (Col. 2 lines 6-24 FIG. 1 shows techniques presently used to increase security in networks that are accessible via the Internet. FIG. 1 shows network 101, which is made up of two separate internal networks 103(A) and 103(B) that are connected by Internet 111. Networks 103(A) and 103(B) are not generally accessible, but are part of the Internet in the sense that computer systems in these networks have Internet addresses and employ Internet protocols to exchange information. Two such computer systems appear in FIG. 1 as requestor 105 in network 103(A) and server 113 in network 103(b). Requestor 105 is requesting access to data which can be provided by server 113. Attached to server 113 is a mass storage device 115 that contains data 117 which is being requested by requester 105. Of course, for other data, server 113 may be the requester and requestor 105 the server. Moreover, access is to be understood in the present context as any operation which can read or change data stored on server 113 or which can change the state of server 113. In making the request, requestor 105 is using one of the standard TCP/IP protocols. As used here, a protocol is a description of a set of messages that can be used to exchange information between computer systems. The actual messages that are sent between computer systems that are communicating according to a protocol are collectively termed a session. During the session, Requestor 105 sends messages according to the protocol to server 113's Internet address and server 113 sends messages according to the protocol to requester 105's Internet address. Both the request and response will travel between internal network 103(A) and 103(B) by Internet 111. If server 113 permits requestor 105 to access the data, some of the messages flowing from server 113 to requestor 105 in the session will include the requested data 117. The software components of server 113 which respond to the messages as required by the protocol are termed a service.)

Referring to claim 37

Referring to claim 3 Schneider and Ross disclose all the limitations of claim 37 which is described above. Schneider also discloses wherein the operations further comprise; transmitting the execution results in response to determining that the storage section stores execution results for a previous execution of the object. (Col 5 lines 56-61 Object Cache 250. The object cache contains the responses to previously submitted requests. All items in the cache are marked with an expiration time that is set at the time they are originally retrieved. The purpose of this layer is to reduce the load on the application tier).

Referring to claim 38

Referring to claim 38 Schneider and Ross disclose all the limitations of claim 38 which is described above. Schneider also discloses passing the call request with respect to the object executor in response to determining that the storage section does not store execution results for the previous execution of the object. (Col.9 lines 40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which data base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information resources 320, which defines the individual information items subject to protection and specifies where to find them; information sets 321, which defines groups of information resources)

Referring to claim 39

Referring to claim 27 Schneider discloses a computer readable storage medium which stores a program for causing a computer system to function as a server unit for providing Web services through a network, said program causes said computer system to perform the steps of: receiving and storing an object call request; acquiring access authority for a request object from memory; reading an access authority set for execution of said request object from the memory (Col. 2 lines 6-24 FIG. 1 shows techniques presently used to increase security in networks that are accessible via the Internet. FIG. 1 shows network 101, which is made up of two separate internal networks 103(A) and 103(B) that are connected by Internet 111. Networks 103(A) and 103(B) are not generally accessible, but are part of the Internet in the sense that computer systems in these networks have Internet addresses and employ Internet protocols to exchange information. Two such computer systems appear in FIG. 1 as requestor 105 in network 103(A) and server 113 in network 103(b). Requestor 105 is requesting access to data which can be provided by server 113. Attached to server 113 is a mass storage device 115 that contains data 117 which is being requested by requester 105. Of course, for other data, server 113 may be the requester and requestor 105 the server. Moreover, access is to be understood in the present context as any operation which can read or change data stored on server 113 or which can change the state of server 113. In making the request, requestor 105 is using one of the standard TCP/IP protocols. As used here, a protocol is a description of a set of messages that can be used to exchange information between computer systems. The actual messages that are sent between computer systems that are communicating according to a protocol are collectively termed a session. During the session, Requestor 105 sends messages according to the protocol to server 113's Internet address and server 113 sends messages according to the protocol to requester 105's Internet address. Both the request and response will travel between internal network 103(A) and 103(B) by Internet 111. If server 113 permits requestor 105 to access the data, some of the messages flowing from server 113 to requestor 105 in the session will include the requested data 117. The software components of server 113 which respond to the messages as required by the protocol are termed a service.); Schneider did not disclose determining whether said access authority is contained in said access authority set; and if said authority is contained in said access authority set, prior to executing said application, searching a storage section which stores execution results for a previous object. The general concept of determining whether said access authority is contained in said access authority set; and if said authority is contained in said access authority set, prior to executing said application, searching a storage section which stores execution results for a previous object is well known in the art as taught by Ross. Ross discloses determining whether said access authority is contained in said access authority set; and if said authority is contained in said access authority set, prior to executing said application, searching a storage section which stores execution results for a previous object(Col 5 lines 56-61 Object Cache 250. The object cache contains the responses to previously submitted requests. All items in the cache are marked with an expiration time that is set at the time they are originally retrieved. The purpose of this layer is to reduce the load on the application tier). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Schneider to include determining whether said access authority is contained in said access authority set; and if said authority is contained in said access authority set, prior to executing said application, searching a storage section which stores execution results for a previous object in order to provide its Hosts with the added value and incremental revenues of traditional affiliate programs, but the company also enables Hosts to control the customer experience before, during, and after the purchase transaction.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashley d. Turner whose telephone number is 571-270-1603. The examiner can normally be reached on Monday thru Friday 7:30a.m. - 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached at 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-270-2603.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Patent Examiner: Supervisory Patent
Examiner

__________________ ____________________

Ashley Turner Nathan Flynn

Date:________ Date:_______

/Nathan J. Flynn/

Supervisory Patent Examiner, Art Unit 2154